Cassandra Crossing/ Dopo Truecrypt

(357)—E' trascorso oltre un anno da quando la confusione è calata su Truecrypt, sono nati fork e sono state condotte analisi sul codice…

Cassandra Crossing/ Dopo Truecrypt

Figure 1:

(357)—E' trascorso oltre un anno da quando la confusione è calata su Truecrypt, sono nati fork e sono state condotte analisi sul codice. Ora di chi ci si può fidare?

2 ottobre 2015—La coazione a ripetere che notoriamente affligge Cassandra, unita ad un paio di decenni passati ad addestrare giovani menti a farsi le domande migliori, la obbliga, per l'afflizione dei suoi 24 indefettibili lettori, a tornare sull'argomento Truecrypt, il noto software di cifratura di disco, progetto open source considerato il top ma abbandonato improvvisamente dai suoi sviluppatori, oggetto di un takeover di dubbissima reputazione.

Lo trovate qui e non assolutamente qui per i motivi che trovate in questo articolo (la 7.1a va bene, la 7.2 NO!). Dopo questa lunghissima premessa, perché riparlarne?

Per due ottimi motivi: il primo è un recentissimo articolo su due bug trovati nel codice originale di Truecrypt (data l'importanza lo ripetiamo, la 7.1a, l'unica versione da prendere in considerazione, mai usare la cosiddetta 7.2), il secondo è la necessità di riassumere in maniera sintetica cosa è successo a Truecrypt, ai software simili ed ai suoi derivati dopo oltre un anno.

Ovviamente sono solo opinioni e profezie di Cassandra, per cui fatene l'uso che ritenete.

Una premessa: se volete usare un software di cifratura del disco, quale è il vostro modello di minaccia? Non nel senso tecnico, troppo complesso per questo contesto, ma più terra-terra. Cifrate il disco: da chi dovete difendervi?

Dal fidanzato/fidanzata geloso/a che vorrebbe vedere le foto che scattate e non gli/le fate vedere, leggere le vostre mail o trovare la password dei vostri social account?

Da un bravo consulente informatico in grado di eseguire analisi forense, pagato dalla persona del punto precedente, o da altri?

Da un servizio segreto, da un pool di investigazione bene attrezzato, da una mafia di varia nazionalità od altra organizzazione criminale?

Nel primo modello di minaccia, qualunque software di cifratura va probabilmente bene.

Nel secondo vi serve un software affidabile, usato ovviamente con competenza, cura ed attenzione.

Nel terzo… Beh, ovviamente lasciate perdere, niente illusioni. Concentriamoci quindi sul secondo caso: vi serve un prodotto affidabile, di buona reputazione, open source, soggetto a controlli di terzi e dimostratamente solido.

Dobbiamo scartare quindi oggetti come Bestcrypt, della Jetico (altra ditta dalla storia "strana") ed ovviamente anche la funzionalità Bitlocker di Windows 8 Professional e le equivalenti di altri sistemi operativi closed source.

Escludendo Truecrypt 7.2 (versione taroccata), solo restano i fork e le reimplementazioni di Truecrypt 7.1a (ben descritti in questo interessante thread) che sono:- TCNext- CipherShed- GostCrypt- VeraCrypt.

Scartiamo subito (almeno per ora) TCNext e CypherShed, che sono iniziative che non hanno ancora rilasciato (e forse non lo faranno mai) un'applicazione stabile.Scartiamo, per motivi diversi, il curioso GostCrypt, il cui tratto distintivo è aver sostituito qua e là agli algoritmi occidentali (NSA, IBM etc) i corrispondenti algoritmi russi.

Resta Veracrypt, l'unico porting che ha rilasciato software stabile (oddio, con tanti problemi di gioventù, comunque) e multipiattaforma, sviluppato da una piccola software house chiamata IDRIX ed ospitato da Codeplex di Google.

Tiriamo le somme. Da una parte abbiamo Veracypt un programma giovane, ancora non verificato da entità indipendenti, e che non offre praticamente niente in più rispetto a Truecrypt, se non un ambiente di sviluppo vivo e (si dice) più moderno.

Dall'altra abbiamo il non più sviluppato Truecrypt 7.1a, il cui codice è disponibile ed auditato totalmente o parzialmente da ben due diverse iniziative, che hanno trovato solo due bachi degni di nota. Sono nella versione Windows, e possono portare ad un escalation di privilegi ed alla lettura della password in memoria.

Però dovete essere collegati come amministratori, avere la partizione montata ed aver lasciato la macchina non bloccata o infettata da qualche malware che ne consenta il controllo remoto. Eventualità improbabile, e comunque al di fuori di un uso appena appena accorto.

Truecrypt 7.1a è un'applicazione che fa quello che deve fare, lo fa bene e non necessita di ulteriori sviluppi. Non avrà problemi fino a quando, in seguito a imprevedibili sviluppi futuri dei sistemi operativi supportati, il codice ormai congelato potrà divenire non compilabile.

Per ora la versione Windows ha retto due major release senza problemi (Windows 8 e 10) e quella Linux 4 major release del kernel.

La risposta quindi è facile: tenetevi Truecrypt 7.1a fino a quando non si presentino problemi di compatibilità con nuove versioni di sistemi operativi.Allora forse qualcuno patcherà il codice

e potrete continuare ad aggiornare il vostro sistema operativo, oppure switchare su Veracrypt, se le condizioni future lo renderanno affidabile.

Ma, come dettagliatamente spiegato nel precedente articolo il legittimo successore di Truecrypt 7.1a dovrebbe essere LUKS, ancora però mal supportato da Windows.

Curiosamente, ma nemmeno poi tanto, Matt Jancer, in un articolo apparso su Wired di settembre (solo edizione cartacea), con meno motivazioni tecniche raggiunge le stesse conclusioni che Cassandra ha sempre sostenuto e continua a sostenere.

Tenetevi Truecrypt 7.1a.

Originally published at punto-informatico.it.

Nota per che riceve gli articoli via mail. *Medium.com modifica automaticamente i link contenuti negli articoli quando li invia per mail, rendendoli traccianti.* ***La cosa disgusta Cassandra****, che se ne è accorta solo di recente grazie ad una provvidenziale segnalazione. Se ciò superasse il vostro limite di indignazione, ed in attesa che Cassandra trovi una soluzione od un'alternativa, potete fruire dell'articolo direttamente sul sito.*

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on November 22, 2023.

Canonical link

Exported from Medium on August 27, 2025.